arXiv:1504.00388v2 [quant-ph] 28 Jan 2016

Symmetric extendibility of quantum states

Marcin L. Nowakowski
Faculty of Applied Physics and Mathematics, Gdansk University of Technology, 80-952 Gdansk, Poland and National Quantum Information Center of Gdansk, Andersa 27, 81-824 Sopot, Poland

Studies on symmetric extendibility of quantum states become especially important in a context of analysis of one-way quantum measures of entanglement, distilabillity and security of quantum protocols. In this paper we analyse composite systems containing a symmetric extendible part with a particular attention devoted to one-way security of such systems. Further, we introduce a new one-way monotone based on the best symmetric approximation of quantum state. We underpin those results with geometric observations on structures of multi-party settings which posses in sub-spaces substantial symmetric extendible components. Finally, we state a very important conjecture linking symmetric-extendibility with one-way distillability and security of all quantum states analyzing behavior of private key in neighborhood of symmetric extendible states.

PACS numbers: 03.67.-a, 03.67.Hk

I. INTRODUCTION

Recent years have proved a great interest of symmetric extendibility concept showing its usability in quantum communication theory, especially in domain of one-way communication. A natural relation between monogamy of entanglement and symmetric extendibility concept was established [1–3] with an important application to analysis of Bell inequalities for multipartite settings where some of the parties possess the same sets of measurement settings. Further, the concept is central for studies of one-way quantum channel capacities, entanglement distillability and private key analysis deriving new upper bounds on these communication rates [4–7, 18, 19]. It seems also that symmetric extendibility is fundamental for studies on recovery and entanglement breaking channels including its neighborhood [10] as well as for such measures like squashed entanglement and quantum discord [22] or analysis of directed communication in 1D/2D spin chains [17]. The aforementioned applications sufficiently prove importance of the notion for quantum communication theory. The challenge for the present quantum information theory in domain of one-way communication is to better understand behavior of all quantum states in the region of non-symmetric extendibility and in particular in a region of non-positive coherent information [8] where no known one-way protocol for distillation of entanglement and private key exists. We believe that the following paper will support these studies. In this paper we provide some new observations about behavior of symmetric states under action of one-way LOCC operations and remind important facts about composite systems containing a symmetric extendible part. Further, we analyze a concept of locking non-symmetric extendibility with its application for security of quantum states asking abut behavior of states assisted by symmetric extendible part. Moreover, we derive a very important link between all two-qubit states not being extendible and one-way entanglement distillation and privacy, analyzing also behavior of private key in neighborhood of symmetric extendible states. In this context, we verified non-symmetric extendible two-qubit Werner states in the region of non-positive coherent information [26] putting an important question about their distillability or existence of one-way bound entanglement. We also give a formalized structure to some natural intuitions about nature of composite systems and its reference to k-extendible states.

II. SYMMETRIC EXTENDIBLE STATES

Particularly symmetric extendibility [1–3] of a given bipartite state $\rho_{AB} \in B(\mathcal{H}_A \otimes \mathcal{H}_B)$ denotes that there exists a tripartite state $\rho_{ABE} \in B(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_B)$ invariant due to permutation of B and E part, namely, if:

$$P = \sum_{ijk} |ijk\rangle\langle ikj| \tag{1}$$

then $P\rho_{ABE}P^\dagger = \rho_{ABE}$ and $Tr_E\rho_{ABE} = \rho_{AB} = \rho_{AE}$.

By 0-extendible states we will denote those that are not symmetrically extendible at all. One could note that it might be useful to partition the set of all symmetric extendible states SE by relation of k-extendibility. If $\mathcal{S}_k$ denotes a convex set [18] of all states being k-extendible, there holds the natural inclusion relation [Fig. 1]:

$$\mathcal{S}_1 \supset \mathcal{S}_2 \supset \ldots \supset \mathcal{S}_k \tag{2}$$

Of a great importance is the fact that for a given $\rho_{AB} \in SE$ there may exist different k-rank symmetric extensions so that the property is not unique and one could represent the set of appropriate symmetric extensions by means of equivalence classes given by the relation $B(\mathcal{H}_A \otimes \mathcal{H}_B) \ni \rho_{AB} \sim \rho \in B(\mathcal{H}_A \otimes \mathcal{H}_B^{\otimes(k+1)})$ if and only if ρ is a k-rank symmetric extension of state ρ_{AB}. As the trivial example note that for $\rho_{AB} = \frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|)$ at least the following are extensions of rank one: $|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ and $\rho = \frac{1}{2}(|000\rangle\langle 000| + |111\rangle\langle 111|)$.

For k-extendible states it might be useful to introduce

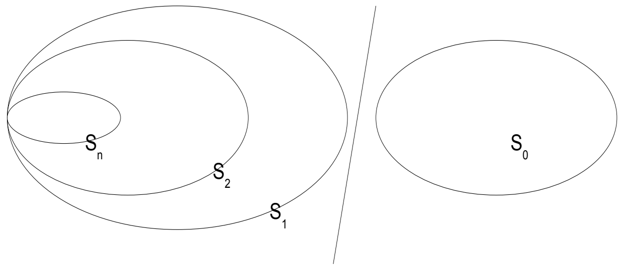

FIG. 1: The space of quantum states can be decomposed by the relation of k-extendibility. $\mathcal{S}_0$ denotes the set of all non-extendible states whereas $\mathcal{S}_n$ the set of states having n-rank symmetric extensions.

an operator swapping $k+1$ particles:

$$P_\pi = \sum_{i_1 i_2 \ldots i_{k+1}} |i_1 i_2 \ldots i_{k+1}\rangle\langle \pi(i_1)\pi(i_2)\ldots\pi(i_{k+1})| \quad (3)$$

where swapping is performed for an arbitrary permutation π. Hence, there holds a general relation for k-extendibility that explicitly derives set $\mathcal{S}_k$: $\forall_\pi \; P_\pi \rho_{AB_1\ldots B_k B_{k+1}} P_\pi^\dagger = \rho_{AB_1\ldots B_k B_{k+1}}$.

Example 1. As a 1-extendible state we present $\rho_{AB} = \frac{1}{3}|00\rangle\langle 00| + \frac{2}{3}|\Phi_+\rangle\langle\Phi_+|$ that obviously possess rank-1 symmetric purification to W-state $|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$.

We could derive for this example a general form of n-extendible state inheriting from W-like n-partite states:

$$\Upsilon_{AB}(n) = \frac{n}{n+2}|00\rangle\langle 00| + \frac{2}{n+2}|\Phi_+\rangle\langle\Phi_+| \quad (4)$$

where $|\Phi_+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$. Interestingly one can simply show that for e.g. GHZ-like n-partite states being a maximal extension of $\rho_{AB} = \frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|)$ there holds $\rho_{AB} = \lim_{n\to\infty}\rho_{AB}(n)$ that is in agreement with theorems [3] stating implicitly that ρ is separable if and only if is ∞-extendible (where $\rho_{AB}(n)$ is derived from n-partite GHZ state).

Following we present two different approaches to the problem of representation of symmetric extensions in extended space. The first approach is widely used in previous papers (see [1–3]) on extendibility of quantum states. Every bipartite state $\rho_{AB} \in B(\mathcal{H}_A \otimes \mathcal{H}_B)$ where $\mathcal{H}_A = \mathbb{C}^m$ and $\mathcal{H}_B = \mathbb{C}^n$ can be represented in the basis of generators of group $SU(m)\otimes SU(n)$ as follows:

$$\begin{aligned}\rho_{AB} \;=\; & \gamma\sigma_A^0 \otimes \sigma_B^0 + \sum_i \alpha_i \sigma_A^0 \otimes \sigma_B^i + \quad (5)\\ & + \sum_j \beta_j \sigma_A^j \otimes \sigma_B^0 + \sum_{i,j\neq 0} \zeta_{ij}\sigma_A^i \otimes \sigma_B^j\end{aligned}$$

where σ_B^i are basis elements of $SU(n)$ and respectively σ_A^i for $SU(m)$. Elements of the basis satisfy relations: $Tr[\sigma_S^i \sigma_S^j] = \eta_S \delta_{ij}$ and $Tr[\sigma_S^i] = \delta_{1i}$ with $S = \{A, B\}$. Therefore, one could derive a general representation of all 1-rank symmetric extensions:

$$\begin{aligned}\rho_{AB_1B_2} \;=\; & \sum_{i,j\neq 0} \alpha_{ij}\sigma_A^i \otimes \sigma_{B_1}^j \otimes \sigma_{B_2}^j + \quad (6)\\ & + \sum_{ijk, j<k} \beta_{ijk}(\sigma_A^i \otimes \sigma_{B_1}^j \otimes \sigma_{B_2}^k + \sigma_A^i \otimes \sigma_{B_1}^k \otimes \sigma_{B_2}^j)\end{aligned}$$

and further, for general case of k-extendibility:

$$\begin{aligned}\rho_{AB_1\ldots B_{k+1}} = & \sum_{i,j\neq 0} \alpha_{ij}\sigma_A^i \otimes \sigma_{B_1}^j \otimes \ldots \otimes \sigma_{B_{k+1}}^j + \quad (7)\\ & \sum_{i,i_1<i_2<\ldots<i_{k+1}} \sum_\sigma \beta_{ii_1\ldots i_{k+1}} \sigma_A^i \otimes \sigma_{B_1}^{\sigma(i_1)} \otimes \ldots \otimes \sigma_{B_{k+1}}^{\sigma(i_{k+1})}\end{aligned}$$

The latter approach that we will utilize in this paper is based on partitioning a space on which Bobs' states operate into symmetric and antisymmetric subspace.

Following we will prove some lemmas about Schmidt decomposition of k-rank pure symmetric states that supports in course of the paper more powerful theorem about properties of symmetric extendible states.

Lemma II.1. *Let $\rho_{AB_1} \in B(\mathcal{H}_A \otimes \mathcal{H}_{B_1})$ be symmetrically extendible to a k-rank pure extension $\Psi_{AB_1\ldots B_{k+1}} \in \mathcal{H}_A \otimes \mathcal{H}_{B_1}^{\otimes k+1}$ then there exists a Schmidt decomposition:*

$$\Psi_{AB_1\ldots B_{k+1}} = \sum_i \alpha_i |\phi_i^{AB_1}\rangle|\psi_i^{B_{2\ldots k+1}}\rangle \quad (8)$$

where $\{|\phi_i^{AB_1}\rangle\}, \{|\psi_i^{B_{2\ldots k+1}}\rangle\}$ are orthonormal sets and $|\psi_i^{B_{2\ldots k+1}}\rangle \in Sym^k \bigoplus Asym^k(\mathcal{H}_{B_1})$.

Proof. Since:

$$\forall_\pi \; I_{AB_1} \otimes P_\pi \Psi_{AB_1\ldots B_{k+1}} = \pm\Psi_{AB_1\ldots B_{k+1}}$$

where P_π operates only on $B_2 \ldots B_{k+1}$ of the system, then $\sum_i \alpha_i |\phi_i^{AB_1}\rangle P_\pi |\psi_i^{B_{2\ldots k+1}}\rangle = \pm\sum_i \alpha_i |\phi_i^{AB_1}\rangle|\psi_i^{B_{2\ldots k+1}}\rangle$. However, since the state is a symmetric extension, the above Schmidt decomposition is invariant due to any permutation on B-part and $|\phi_i^{AB_1}\rangle$ indexes uniquely the $|\psi_i^{B_{2\ldots k+1}}\rangle$ states so P_π transforms $|\psi_i^{B_{2\ldots k+1}}\rangle$ onto itself. Therefore, the second multiplicands of Schmidt decomposition represent either symmetric or antisymmetric orthonormal states. □

When in [4] spectral conditions for 1-rank symmetric extensions were stated, following we derive general statement about spectral conditions for k-extendible states basing on the observation about decomposition of symmetric states.

Observation II.2. *Every pure normalized state* $|\Psi\rangle \in Sym^{k+1} \bigoplus Asym^{k+1}(\mathcal{H}_{B_1})$ *of k+1-partite system can be decomposed to the following Schmidt form:*

$$\forall_{1<l<k}|\Psi\rangle = \sum_i |\phi_i^{B_1 \ldots B_l}\rangle|\phi_i^{B_{l+1}\ldots B_{k+1}}\rangle$$

where the multiplicands form respectively symmetric or antisymmetric orthonormal sets.

Proof. One can conduct the proof similarly to $(II.1)$. Since $\forall_\pi P_\pi|\Psi\rangle\langle\Psi|P_\pi = |\Psi\rangle\langle\Psi|$, then for all possible permutations the operation cannot change Schmidt decomposition of $\sum_i |\phi_i^{B_1\ldots B_l}\rangle|\phi_i^{B_{l+1}\ldots B_{k+1}}\rangle$. Furthermore, due to assumed symmetry property of $|\Psi\rangle$, a state of any l-subsystem $B_1 \ldots B_l$ represented by the first multiplicand is permutationally invariant and the same is applied to the second multiplicand. □

This observation with application of lemma II.1 can be effectively used to generate k-extendible states.

Observation II.3. *Let* ρ_{AB_1} *be k-extendible to a pure symmetric state* $|\Psi\rangle_{AB_1\ldots B_{k+1}}$ *then for ordered vectors of eigenvalues of* ρ_{AB_1} *and* $\rho_{B_2\ldots B_{k+1}}$ *there holds:*

$$\lambda^{\downarrow}(\rho_{AB_1}) = \lambda^{\downarrow}(\rho_{B_2\ldots B_{k+1}}) \tag{9}$$

Proof. The proof is immediate applying Schmidt decomposition and results of (II.1). □

III. SYMMETRIC EXTENDIBILITY OF COMPOSITE SYSTEMS

In this section we explore symmetric extendibility of complex systems consisting of n pairs. All following statements are vital for protocols acting on multiple pairs of states.

For further results of the following section we will present a generalized version of a lemma [18] up to k-extendible maps stating that no matter what operation Alice and Bob can perform, the symmetric state shared between Alice and Bob will keep its symmetric extendibility. The following lemma indicates a natural fact that one cannot produce k-extendible state from n-extendible state $(n > k)$ by means of 1-LOCC $\Lambda_{\rightarrow}(\cdot)$ even if acts on any number of pairs:

Lemma III.1. *Let* $\Lambda_{\rightarrow}$ *be a 1-LOCC quantum operation (not necessarily trace-preserving):*

$$\Lambda_{\rightarrow}(\rho) = \sum_{ij}(I\otimes B_{ij})(A_i\otimes I)\rho(A_i\otimes I)^\dagger(I\otimes B_{ij})^\dagger$$

where $\sum_i A_iA_i^\dagger \leq I$ *and* $\sum_j B_{ij}B_{ij}^\dagger = I$ *for all i since Bob cannot communicate the outcome of a probabilistic operation back to Alice. If* ρ *is k-extendible state then* $\Lambda_{\rightarrow}(\rho)$ *is n-extendible and* $n \geq k$.

One may state a non-trivial question if it is feasible to achieve symmetric extendibility of a composition of quantum states when at least one of them is not-symmetric extendible. The result of this question is crucial both for quantum security applications and measuring quantum entanglement. The following lemma casts some light on this field:

Lemma III.2. *If* $\rho_{AB} \in B(\mathcal{H}_A^N \otimes \mathcal{H}_B^M)$ *is not symmetrically extendible state then there does not exist any such a state* $\rho_{A'B'} \in B(\mathcal{H}_{A'}^K \otimes \mathcal{H}_{B'}^L)$ *that* $\rho_{AB}\otimes\rho_{A'B'}$ *would be symmetrically extendible in respect to* BB' *subsystem.*

Proof. Conversely, let $\rho_{ABA'B'} = \rho_{AB}\otimes\rho_{A'B'}$ be a symmetrically extendible state acting on $B(\mathcal{H}_A^N \otimes \mathcal{H}_B^M \otimes \mathcal{H}_{A'}^K \otimes \mathcal{H}_{B'}^L)$. Therefore, one notes that $\rho_{ABA'B'}$ after swapping to $\rho_{AA'BB'}$ can be represented by method (5) in an appropriate basis including generators of group $SU(N)\otimes SU(K)\otimes SU(M)\otimes SU(L)$ and further, can be extended to a 1-rank symmetric extension $\rho_{AA'BB'\widetilde{B}\widetilde{B'}}$ where we extend BB' part as follows:

$$\begin{aligned}\rho_{AA'BB'\widetilde{B}\widetilde{B'}} &= \sum_{ijkl}\alpha_{ijkl}T_{ijklkl} + \\ &+ \sum_{ijklmn}\beta_{ijklmn}(T_{ijklmn}+T_{ijmnkl})\end{aligned} \tag{10}$$

with tensors $T_{ijklmn} = \sigma^i\otimes\sigma^j\otimes\sigma^k\otimes\sigma^l\otimes\sigma^m\otimes\sigma^n$. Following we derive the state $\rho_{AB\widetilde{B}}$ of system $AB\widetilde{B}$ tracing out that of $A'B'\widetilde{B'}$. For the fact that $Tr[\sigma^i\otimes\sigma^j\otimes\sigma^k] = Tr(\sigma^i)Tr(\sigma^j)Tr(\sigma^k)$ and $Tr[\sigma^i] = \delta_{1i}$ after tracing out only elements with $\sigma^0 = I$ remain, namely, one obtains:

$$\begin{aligned}\rho_{AB\widetilde{B}} &= \sum_{ik}\alpha_{i1k1}T_{i1k1k1} + \\ &+ \sum_{ikm}\beta_{i1k1m1}(T_{i1k1m1}+T_{i1m1k1})\end{aligned} \tag{11}$$

Hence, $\rho_{AB\widetilde{B}}$ is 1-rank symmetric extension of ρ_{AB} that is in contradiction with the assumption that the latter is not symmetrically extendible. □

Corollary III.3. *If* $\rho_{AB} \in B(\mathcal{H}_A^N \otimes \mathcal{H}_B^M)$ *is at most k-extendible state then there does not exist any such a state* $\rho_{A'B'} \in B(\mathcal{H}_{A'}^K \otimes \mathcal{H}_{B'}^L)$ *that* $\rho_{AB}\otimes\rho_{A'B'}$ *would be k+1-extendible in respect to* BB' *subsystem.*

Lemma III.4. *Assume that* $\rho_{AB} \in B(\mathcal{H}_A\otimes\mathcal{H}_B)$ *is not symmetric extendible and there exists a local operation* $\mathbb{F}$ *acting on A-part such that* $\sigma_{AB} = (\mathbb{F}\otimes id)\rho_{AB}(\mathbb{F}^\dagger\otimes id)/Tr[(\mathbb{F}\otimes id)\rho_{AB}(\mathbb{F}^\dagger\otimes id)]$ *is a symmetric extendible state.*

Then for any local operations $\mathbb{A}$ *and* $\mathbb{B}$ *acting on A and B part of the system:*

$$\mathbb{A} = U\begin{pmatrix}\alpha_0 & & & \\ & \alpha_1 & & \\ & & \ddots & \\ & & & \alpha_i\end{pmatrix}U^\dagger \tag{12}$$

$$\Lambda(\rho_{AB}) = \frac{\mathbb{A}\otimes\mathbb{B}\rho_{AB}\mathbb{A}^\dagger\otimes\mathbb{B}^\dagger}{Tr(\mathbb{A}\otimes\mathbb{B}\rho_{AB}\mathbb{A}^\dagger\otimes\mathbb{B}^\dagger)} \tag{13}$$

where for all i $0 < \alpha_i \leq 1$ and U denotes an unitary operation ($\mathbb{B}$ has a corresponding structure), there exists a local operation $\widetilde{\mathbb{F}}$ such that $\widetilde{\sigma}_{AB} = (\widetilde{\mathbb{F}}\otimes id)\Lambda(\rho_{AB})(\widetilde{\mathbb{F}}^\dagger\otimes id)/Tr[(\widetilde{\mathbb{F}}\otimes id)\Lambda(\rho_{AB})(\widetilde{\mathbb{F}}^\dagger\otimes id)]$ is symmetric extendible and $\dim\mathbb{F} = \dim\widetilde{\mathbb{F}}$.

Proof. To prove this lemma, it suffices to note that $\mathbb{A} = UDU^\dagger$ with a diagonal matrix D. Further, we observe that $\widetilde{\mathbb{F}} = \mathbb{F}\circ UD'U^\dagger$ where $D'D = id$. The latter is possible due to the condition that for all i there holds: $0 < \alpha_i \leq 1$ and we easily observe that $\mathbb{F} = \widetilde{\mathbb{F}}\circ\mathbb{A}$. This brings us to conclusion that $\widetilde{\mathbb{F}}\Lambda(\rho_{AB})\widetilde{\mathbb{F}}^\dagger$ is a symmetric extendible operator (after normalization becoming a physical state). For B-part the proof can be conducted in a similar manner as in particular, the local operation $\mathbb{B}$ is also revertible. □

Remark. It casts some light on a fact that local operations actually does not change the amount of symmetric extendibility embedded in a state.

This lemma is of a great importance for private security and entanglement distillation studies, as we can always build a symmetric extension Γ_{ABE} of a state $\widetilde{\sigma}_{AB}$ which means that Eve potentially has a state $\rho_E = \rho_B = Tr_A\widetilde{\sigma}_{AB}$ and operates on such a space. To support this statement one can further derive the corollary about extendibility of any quantum state with a proposal of new extendible number of a quantum state:

Definition III.5. *For any ρ_{AB}, $\eta_{SE}(\rho_{AB}) = \max_{\mathbb{F}}\dim\mathbb{F}$ is called the extendible number of a state ρ_{AB} where $(\mathbb{F}\otimes id)\rho_{AB}(\mathbb{F}^\dagger\otimes id)$ is a symmetric extendible operator and $\mathbb{F}$ is a local operation acting on A.*

Corollary III.6. *Any state $\rho_{AB}\in B(\mathcal{H}_A\otimes\mathcal{H}_B)$ with extendible number η_{SE} can be extended to a state $\rho_{ABE}\in B(\mathcal{H}_A\otimes\mathcal{H}_B\otimes\mathcal{H}_E)(\dim\mathcal{H}_B = \dim\mathcal{H}_E)$ where exists filtering operation $\mathbb{F}$ on A so that $(\mathbb{F}\otimes id)\rho_{ABE}(\mathbb{F}^\dagger\otimes id)$ is invariant due to permutation of B and E.*

Naturally, there holds: if $\eta_{SE}(\rho_{AB}) = rank(\rho_A)$, then the state is symmetric extendible.

One may raise further a very important question how to create the property of symmetric non-extendibility both in case of single states and collective systems using only local operations or additionally one-way communication that naturally will have implications for distillability and capacities of corresponding states and channels.

Lemma III.7. *Let $\rho_{AB}\in B(\mathcal{H}_{AB})$ be a state possessing at most k-rank symmetric extension where $k<\infty$ then there does not exist any 1-LOCC protocol represented by $\Lambda_{A\to BC} : B(\mathcal{H}_{ABC}) \to (\widetilde{\mathcal{H}}_{ABC})$ (not necessarily trace-preserving):*

$$\Lambda_{A\to BC}(\rho_{AB}\otimes\sigma_C) = \widetilde{\rho}_{ABC} \tag{14}$$

so that $\widetilde{\rho}_{ABC}$ is a symmetric extension of ρ_{AB} and $\sigma_C\in B(\mathcal{H}_C)$ is an additional resource on Bob's side.

Proof. Since ρ_{AB} is k-extendible, one can assume that its symmetric extension is realized to $\rho_{ABB_1\ldots B_k}$ but $B_1\ldots B_K$-part is possessed by Eve. Obviously no communication between Eve and Bob in such a scenario is allowed so that Bob cannot detect locally Eve and further, since the set of symmetric extendible states is closed under $1-LOCC$ operations [18] even if Alice and Bob had engaged one-way communication they cannot break symmetric extendability of ρ_{AB} and so cannot eliminate Eve if the symmetric extension had been realized.

Therefore, assuming that on the contrary $\Lambda_{A\to BC}$ enables creation of a symmetric extension:

$$\Lambda_{A\to BC}\otimes id_{B_1\ldots B_k}(\rho_{ABB_1\ldots B_k}\otimes\sigma_C) = \Omega \tag{15}$$

resulting state Ω would be k+1-symmetric extension of ρ_{AB} that contradicts the lemma's assumption about extendibility of this state and completes the proof. □

Remark. The aforementioned statements holds as well in asymptotic regime due to results of III.2 that can be extended for an infinite case.

As a result of the above lemmas we can conclude that in general for creation of any symmetric extension one needs to engage two-way communication.

IV. SYMMETRIC EXTENDIBLE COMPONENT IN QUANTUM STATES

In this section we consider vulnerability of quantum states to the loss of non-symmetric extendibility property asking how easily the quantum state becomes symmetric extendible by distraction of its sub-system or how much of symmetric extendibility can be extracted from the state. When the former recalls lockability of entanglement, the latter relates to the best symmetric approximation subject responding to the question: how much of non-symmetric extendible component has to be mixed with symmetric extendible state so that it becomes non-symmetric extendible?

The general idea of locking a property of a quantum state relates to the loss or decrease of this property subjected to a measurement or discarding of one qubit. It has been shown [14, 25] that entanglement of formation, entanglement cost and logarithmic negativity are lockable measures which manifests as an arbitrary decrease of those measures after measuring one qubit.

Herewith, we analyze in fact locking of non-symmetric extendibility in sense that discarding one qubit from the quantum state that is not symmetric extendible leads to the loss of this property. Further, we derive implications for quantum security applying one-way communication between engaged parties Alice and Bob.

We shall show now that the property of non-symmetric extendibility of an arbitrary state ρ_{AB} can be destroyed by measurement of one qubit and in result it presents

how easily a quantum state can be removed of one-way distillability and security.

Let us consider bipartite quantum state shared between Alice and Bob on the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B \cong \mathcal{C}^{d+2} \otimes \mathcal{C}^{d+2}$

$$\rho_{AB} = \frac{1}{2d-1} \begin{bmatrix} dP_+ & 0 & 0 & \mathcal{A} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \mathcal{A}^\dagger & 0 & 0 & \sigma \end{bmatrix} \tag{16}$$

where P_+ is a maximally entangled state on $\mathcal{C}^d \otimes \mathcal{C}^d$, $\sigma = \sum_{i=1}^{d-1} |i\ 0\rangle\langle i\ 0|$ and $\mathcal{A}$ is an arbitrary chosen operator so that ρ_{AB} represents a correct quantum state. This matrix is represented in the computational basis $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ held by Alice and Bob and possess a singlet-like structure. Whenever one party (Alice or Bob) measures the state in the local computational basis, the state decoheres and off-diagonal elements vanish which leads to a symmetric extendible state [18]:

$$\Upsilon_{AB} = \frac{d}{2d-1} P_+ + \frac{1}{2d-1} \sum_{i=1}^{d-1} |i\ 0\rangle\langle i\ 0| \tag{17}$$

from which no entanglement nor secret key can be distilled by means of one-way communication and local operations. Clearly this example shows that from a non-symmetric extendible state possessing large entanglement cost and non-zero one-way secret key one can easily obtain a symmetric structure by discarding small part of the whole system destroying possibility of entanglement distillation and secret key generation by means of 1-LOCC.

Thus, it is interesting to consider how much of symmetric extendibility is embedded in a given state ρ_{AB} as it can be expected that the more symmetric extendibility is hidden in a state, the less vulnerable for losses of one-way distillable entanglement and security it is. Besides analysis of symmetric structures in projected subspaces, we will also propose to perform this task by means of *the best symmetric extendible approximation* [6, 20] that decomposes the state into a symmetric extendible component σ_{ext} and non-symmetric extendible component σ_{next}:

$$\rho_{AB} = \max_\lambda \lambda\sigma_{ext} + (1-\lambda)\sigma_{next} \tag{18}$$

We denote by $\lambda_{max}(\rho)$ the maximum weight of extendibility [6] of ρ_{AB} where $0 \leq \lambda_{max}(\rho) \leq 1$,thus, all symmetric extendible states have the weight $\lambda_{max} = 1$. It is proved in [5, 6] that in case of one-way protocols only the non-symmetric extendible component can be effectively utilized for generation of a secret key and it confirms that the notion of symmetric extendibility is crucial for consideration of one-way entanglement and key distillation.

However, we show that there exist states which do not possess any symmetric extendible component in the aforementioned decomposition but there can be a large symmetric extendible component embedded in them. An example of such a state is given above (16) and one can derive the following statement about general structure of such states:

Lemma IV.1. *Consider a state γ on $\mathcal{H}_{AA'BB'} = \mathcal{H}_A \otimes \mathcal{H}_{A'} \otimes \mathcal{H}_B \otimes \mathcal{H}_{B'} \sim \mathcal{C}^d \otimes \mathcal{C}^d \otimes \mathcal{C}^d \otimes \mathcal{C}^d$:*

$$\gamma = \rho \otimes \sigma \tag{19}$$

being a composition of an arbitrary chosen state $\sigma \in B(\mathcal{H}_{A'} \otimes \mathcal{H}_{B'})$ and a non-symmetric extendible state $\rho \in B(\mathcal{H}_A \otimes \mathcal{H}_B)$ with no symmetric extendible component $\lambda_{max}(\rho) = 0$. Then for the best extendible approximation of γ there holds $\lambda_{max}(\gamma) = 0$, i.e. there is no symmetric extendible component in $\gamma \in B(\mathcal{H}_{AA'BB'})$.

Proof. Conversely, assume that there exists decomposition of $\gamma_{AA'BB'}$ with non-zero symmetric extendible component, i.e. $\lambda \neq 0$:

$$\gamma_{AA'BB'} = \lambda\sigma_{ext} + (1-\lambda)\rho_{ne} \tag{20}$$

then both components would be supported on $\mathcal{H}_{AA'BB'}$ and one can search for a decomposition of $\gamma_{AA'BB'}$ after tracing out A'B'-part. Due to additivity of a partial trace operation $\Gamma_X(\cdot) = Tr_X(\cdot)$ we obtain:

$$\Gamma_{A'B'}(\gamma_{AA'BB'}) = \lambda\Gamma_{A'B'}(\sigma_{ext}) + (1-\lambda)\Gamma_{A'B'}(\rho_{ne}) \tag{21}$$

and, further, basing on a symmetric extendibility property of composite systems [18] one derives that tracing out $A'B'$ from σ_{ext} does not destroy its symmetric extendibility and produces symmetric extendible state $\widetilde{\sigma}_{ext}$:

$$\rho = \lambda\widetilde{\sigma}_{ext} + (1-\lambda)\widetilde{\rho}_{ne} \tag{22}$$

Thus, the initial assumption would imply existence of a non-zero symmetric extendible component of the state ρ that contradicts the aforementioned decomposition. □

Following one can make an immediate observation about any private quantum state [15]:

Corollary IV.2. *Any private quantum state $\gamma_{ABA'B'} \in B(\mathcal{H}_{ABA'B'})$:*

$$\gamma_{ABA'B'} = \frac{1}{2} \sum_{i,j=0}^{1} |ii\rangle\langle jj| \otimes U_i \rho_{A'B'} U_j^\dagger \tag{23}$$

does not possess symmetric extendible component, i.e. $\lambda_{max} = 0$.

Remark. The proof is conducted in analogy to the proof of IV.1 but this state represents a twisted composition of singlet and an arbitrary chosen state σ where AB-part is the key part of the state and is not symmetric extendible due to the observation that secure states cannot be symmetric extendible [6].

Basing on previous studies of entanglement measures and importance of symmetric extendible states, we introduce the following best symmetric approximed entanglement monotone (as a counterpart of BSA in [20]):

Proposition IV.3. *For any $\rho \in B(\mathcal{H}_A \otimes \mathcal{H}_B)$ having best symmetric decomposition $\rho_{AB} = \max_\lambda \lambda\sigma_{ext} + (1-\lambda)\sigma_{next}$, the best symmetric approximated entanglement monotone is defined as:*

$$E^{ss}(\rho) = 1 - \lambda_{max}(\rho) \tag{24}$$

Proof. (We will prove that the quantity meets necessary conditions to be an entanglement monotone.)
1. If ρ is separable, i.e. also symmetric extendible, then $\lambda_{max} = 1$ and $E^{ss}(\rho) = 1 - \lambda_{max} = 0$.
2. $E^{ss}(\rho)$ is invariant under local unitary operations since application of local operations U_A and U_B on σ_{ext} leaves it extendible to the third part B', i.e. $E^{ss}(U_A \otimes U_B \rho U_A^\dagger \otimes U_B^\dagger) \geq E^{ss}(\rho)$ and vice versa.
3. For any local POVM V_i, there holds:

$$\begin{aligned} 1 - \lambda_{max}(\rho) &\geq \sum_i (1 - \lambda_i^{\max}(\rho_i) Tr(V_i \rho V_i^\dagger)) \\ &\geq \sum_i E^{ss}(\rho_i) Tr(V_i \rho V_i^\dagger)) \end{aligned}$$

and $\rho_i = V_i \rho V_i^\dagger / Tr(V_i \rho V_i^\dagger)$. □

It is interesting to notice that for two-qubit states on $\mathbb{C}^2 \otimes \mathbb{C}^2$ there holds a non-trival observation about best symmetric approximated decomposition:

$$\rho = \lambda\sigma_{ext} + (1-\lambda)|\Psi\rangle\langle\Psi| \tag{25}$$

with σ_{ext} being a symmetric extendible component that appears in ρ with highest probability. The proof of this observation can be based on BSA with separable components [20] where $\rho = \alpha\sigma_{sep} + (1-\alpha)|\Psi\rangle\langle\Psi|$. As set of separable states is a subset of the convex set of symmetric extendible states, then for any dimension $\alpha \leq \lambda$. Further, due to the fact that any two-qubit state has best separable decomposition into a separable and projective entangled component, we conclude that $\lambda\sigma_{ext} = \alpha\sigma_{sep} + \beta|\Psi\rangle\langle\Psi|$ for arbitrary chosen β.

These propositions can simplify potentially many research problems like analysis of $CHSH$ regions vs. symmetric extendibility of states [21] represented in the steering ellipsoid formalism or just further analysis on security and distillability of all $\mathbb{C}^2 \otimes \mathbb{C}^2$ states.

Following the results of [23], one can immediately propose max-relative entropy monotone based on this decomposition, i.e. $D_{\max}(\sigma \parallel \rho) \equiv \log\min\{\lambda : \sigma \leq \lambda\rho\}$ and $\mathrm{supp}\sigma \subseteq \mathrm{supp}\rho$ with max-relative entropy being interpreted as a probability of finding σ in decompositions of ρ. This leads immediately to $\lambda = \max(2^{-D_{\max}(\sigma_{ext}\|\rho)})$.

An open question is: whether for one-way distillable entanglement we can state that $D_{\rightarrow}(\rho) \leq (1 - \lambda_{max}(\rho)) D_{\rightarrow}(\sigma_{next})$?

V. IMPLICATIONS FOR ONE-WAY ENTANGLEMENT DISTILLABILITY AND PRIVATE KEY

Studies on symmetric extendibility in a context of measures of entanglement like squashed entanglement [25, 26], security of quantum protocols [6] and quantum maps gain a substantial interest. Recently a great attention has been paid to so called k-extendible maps [22, 27, 28] and recovery maps [29, 30] where it is proved that small value of squashed entanglement implies closeness to highly extendible states. These results show importance of symmetric extendibility notion for analysis of one-way quantum communication rates. Inspired by these findings, we propose further an important conjecture about distillability of all non-symmetric extendible states and analyze behavior of a secret key rate in a neighborhood of symmetric extendible states.

Basing on theory of entanglement distillability we state the following conjecture in domain of one-way communication linking it directly with symmetric extendibility of quantum states:

Conjecture V.1. *Any state ρ_{AB} on $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ is one-way distillable if and only if there exists a two-dimensional projector $P : \mathcal{H}_A^n \rightarrow \mathbb{C}^2$ such that for some $n \geq 1$ the state:*

$$\widetilde{\rho}_{AB} = (P \otimes id)\rho_{AB}^{\otimes n}(P \otimes id)^\dagger \tag{26}$$

is not symmetrically extendible.

For a potential proof, it is an immediate observation that one-way distillable quantum states cannot be symmetric extendible [18], yet it is an open question if there exists a two-qubit state that is not at the same time symmetric extendible nor one-way distillable. Since we know conditions for symmetric extendibility of two-qubit states [4, 7], this conjecture if true would simplify analysis of entanglement of two-qubit states and capacity of channels acting on such spaces substantially. On the contrary, if there exist two-qubit states that are neither symmetric extendible nor one-way distillable then they would be one-way counterparts of bound entangled states for two-way distillability in higer dimensions. An analysis of this subject seems to be of a great importance for further studies on quantum secure protocols and structure of entanglement.

As an example, it is worth mentioning Werner states [31] and the hypothesis about NPT bound entangled states [32, 33]. The structure of the Werner states is as follows:

$$\rho_W(\alpha) = \frac{id + \alpha\mathbb{P}}{d^2 + \alpha d} \tag{27}$$

where $\mathbb{P} = \sum_{i,j=0}^{d-1} |ij\rangle\langle ji|$. The state is separable for $1 \geq \alpha \geq -\frac{1}{d}$, NPT for $-\frac{1}{d} > \alpha \geq 1$ and two-way 1-distillable for $-\frac{1}{2} > \alpha \geq -1$. Applying the conditions for symmetric extendibility [7], we found that

for $d = 2$, the state is non-symmetric extendible for $-0.8 \geq \alpha \geq -1$. We analyzed potential one-way distillability of the state for the region of non-symmetric extendible Werner states with non-positive coherent information, namely for $-0.8 \geq \alpha >\cong -0.85559$. The latter condition excludes all those states being distilled by well-known one-way hashing protocol. The analysis was performed for two-copies of the state and over 10^8 random filtering operations on Alice' side and random unitary operations on Bob's side. However, the protocol was not able to distill states with positive coherent information which suffices to distill entanglement with the hashing protocol. Therefore, it is *an open question* if the state is one-way distillable in the region $-0.8 \geq \alpha >\cong -0.85559$ or it is one-way 'bound entangled' which would be a counterpart of bound entanglement concept in two-way communication domain.

As all symmetric extendible state do not posses any private key, we can expect that in close neighborhood to the set of such states all other states can have only a small amount of distillable private key. That would have to be true assuming at least local continuity of private key $K_{\rightarrow}(\cdot)$ in such a neighborhood. To anylyze this subject, we start reminding an important theorem about entropic inequalities for conditional entropies of sufficiently close states in terms of a trace norm:

Theorem V.2. *[24] For any two states ρ_{AB} and $\widetilde{\rho}_{AB}$ on $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$, let $\epsilon \equiv \| \rho_{AB} - \widetilde{\rho}_{AB} \|_1$ and let d_A be the dimension of $\mathcal{H}_A$, then the following estimate holds:*

$$|S(A|B) - S(\widetilde{A}|\widetilde{B})| \leq 4\epsilon \log d_A + 2\eta(1-\epsilon) + 2\eta(\epsilon) \quad (28)$$

In particular, the right hand side of (28) does not explicitly depend on the dimension of $\mathcal{H}_B$.

Further, to generate a secret key between Alice and Bob one can use [8, 9] a general tripartite pure state ρ_{ABE}. Alice engages a particular strategy to perform a quantum measurement (POVM) described by $Q = (Q_x)_{x\in\mathcal{X}}$ which leads to: $\widetilde{\rho}_{ABE} = \sum_x |x\rangle\langle x|_A \otimes Tr_A(\rho_{ABE}(Q_x) \otimes I_{BE})$. Therefore, starting from many copies of ρ_{ABE} we obtain many copies of cqq-states $\widetilde{\rho}_{ABE}$ and we restate the theorem defining one-way secret key $K_{\rightarrow}$:

Theorem 1.[8] *For every state ρ_{ABE}, $K_{\rightarrow}(\rho) = \lim_{n\to\infty} \frac{K^{(1)}_{\rightarrow}(\rho^{\otimes n})}{n}$, with $K^{(1)}_{\rightarrow}(\rho) = \max_{Q,T|X} I(X : B|T) - I(X : E|T)$ where the maximization is over all POVMs $Q = (Q_x)_{x\in\mathcal{X}}$ and channels R such that $T = R(X)$ and the information quantities refer to the state: $\omega_{TABE} = \sum_{t,x} R(t|x)P(x)|t\rangle\langle t|_T \otimes |x\rangle\langle x|_A \otimes Tr_A(\rho_{ABE}(Q_x) \otimes I_{BE})$. The range of the measurement Q and the random variable T may be assumed to be bounded as follows: $|T| \leq d_A^2$ and $|\mathcal{X}| \leq d_A^2$ where T can be taken a (deterministic) function of $\mathcal{X}$.*

Basing one the above results we will prove continuity of the quantity $K^{(1)}_{\rightarrow}(\rho)$ for one copy of a state ρ and further, consider behavior of the measure in the asymptotic regime.

Lemma V.3. *For any two states ρ and $\widetilde{\rho}$ on $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$, let $\epsilon \equiv \| \rho - \widetilde{\rho} \|_1$ and let d_A be the dimension of $\mathcal{H}_A$, then the following estimate holds:*

$$|K^{(1)}_{\rightarrow}(\rho) - K^{(1)}_{\rightarrow}(\widetilde{\rho})| \leq 8\epsilon \log d_A + 4\eta(1-\epsilon) + 4\eta(\epsilon) \quad (29)$$

Proof. One can put for the quantity $K^{(1)}_{\rightarrow}(\rho) = S(BC) - S(ABC) - S(EC) + S(AEC) = -S(A|BC) + S(A|EC)$ and respectively for $\widetilde{\rho}$ there holds $K^{(1)}_{\rightarrow}(\widetilde{\rho}) = -S(\widetilde{A}|\widetilde{BC}) + S(\widetilde{A}|\widetilde{EC})$. Further, engaging the results of (28) it is easy to conduct the following implications for a chain of inequalities:

$$\begin{aligned} & |K^{(1)}_{\rightarrow}(\rho) - K^{(1)}_{\rightarrow}(\widetilde{\rho})| = \\ = \; & |[S(\widetilde{A}|\widetilde{BC}) - S(A|BC)] + [S(A|EC) - S(\widetilde{A}|\widetilde{EC})]| \\ \leq \; & |S(\widetilde{A}|\widetilde{BC}) - S(A|BC)| + |S(A|EC) - S(\widetilde{A}|\widetilde{EC})| \\ \leq \; & 2[4\epsilon \log d_A + 2\eta(1-\epsilon) + 2\eta(\epsilon)] \end{aligned}$$

□

Since it is not possible to distill any secret key by means of one-way communication and local operations from all symmetric extendible states, one can easily derive the following:

Corollary V.4. *For any state ρ on $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$ being in distance ϵ to the nearest symmetric extendible state $\widetilde{\sigma}$ in sense of a trace norm: $\epsilon = \inf_{\sigma\in\Omega} \| \rho - \widetilde{\sigma} \|_1$ where Ω denotes a convex set of symmetric extendible states on $\mathcal{H}_{AB}$, there holds:*

$$K^{(1)}_{\rightarrow}(\rho) \leq 8\epsilon \log d_A + 4\eta(1-\epsilon) + 4\eta(\epsilon) \quad (30)$$

Example 3. As an example of application of the above corollary we will consider two states very close to one another in sense of a trace norm $\| \cdot \|_1$ from which one is symmetric extendible and the another is non-symmetric extendible. This shows that for one-copy applications the theorem can be used operationally to estimate one-way secret key rate of quantum states. Following results of [18], let us consider two arbitrary instances of a state on $\mathcal{H}_{AB} \cong \mathcal{C}^d \otimes \mathcal{C}^d$:

$$\Upsilon(\epsilon) = [\frac{d}{2d-1} + \epsilon/2]P_+ + [\frac{1}{2d-1} - \frac{\epsilon}{2(d-1)}]\sum_{i=1}^{d-1} |i\,0\rangle\langle i\,0| \quad (31)$$

which is non-symmetric extendible for $\epsilon > 0$. Namely, one can put into the inequality (29) two states $\Upsilon(\epsilon = 0)$ and $\Upsilon(\epsilon > 0)$. Since for all symmetric extendible states ρ there holds: $K^{(1)}_{\rightarrow}(\rho) = 0$, then:

$$K^{(1)}_{\rightarrow}(\Upsilon(\epsilon > 0)) \leq 8\epsilon \log d_A + 4\eta(1-\epsilon) + 4\eta(\epsilon).$$

where $\epsilon \leq \frac{2(d_A-1)}{2d_A-1}$.

It is proved [34] that in any open set of distillable states, all asymptotic entanglement measures $E(\rho)$ are continuous as a function of a single copy of ρ, even though

they quantify the entanglement properties of $\rho^{\otimes N}$ in the large N limit.
However, the aforementioned theorem does not cast any light on the behavior of function $K_{\rightarrow}(\cdot)$ on the boundary of a set of all one-way distillable states adjacent to symmetric extendible states just due to the open conjecture V.1. Motivated by this insight we put an open question in the following form for ϵ-neighborhood of symmetric extendible states having zero one-way secret key rate:

Conjecture V.5. *For any state ρ on $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$ being in distance ϵ to the nearest symmetric extendible state $\widetilde{\sigma}$ in sense of a trace norm: $\epsilon = \inf_{\sigma\in\Omega} \parallel \rho - \widetilde{\sigma} \parallel_1$ where Ω denotes a convex set of symmetric extendible states on $\mathcal{H}_{AB}$, there holds:*

$$K_{\rightarrow}(\rho) \leq 8\epsilon \log d_A + 4\eta(1-\epsilon) + 4\eta(\epsilon) \tag{32}$$

VI. CONCLUSIONS

The theory of symmetric extendible states being crucial for analysis of one-way distillability and security of quantum states has still many unsolved problems. In this paper we introduced some new concepts related to classification of all symmetric extendible states and analyzed mainly composite systems including also a symmetric extendible part. In section II. we introduced some observations about the general structure of symmetric extendible states. In section III. we analyzed the structure of composite systems where its part is symmetric extendible and answered a general question of further extendibility of k-extendible states. We introduced a new notion of the extendible number of a quantum state that can be used in further studies on characterization of such states. As presented in the paper, beside analysis of best symmetric extendible decompositions it might be very useful to analyze a maximal symmetric extendible state that can be achieved by filtering on Alice' side. Further, there has been a new one-way monotone based on the best symmetric approximation of quantum state introduced in section IV. treating about the symmetric extendible component embedded in quantum states.

Finally, in section V. we studied also behavior of private key in neighborhood of symmetric extendible states showing that for one-copy a quantum state close to symmetric extendible state can possess only a small amount of private key. One of the most intriguing open question relates to the conjecture about one-way distillability of all two-qubit states which are not symmetric extendible. In consequence, that would simplify substantially full characterization of two-qubit states in terms of their privacy and distillability. In relation to this question we analyzed Werner states in the domain of non-positive coherent information which would indicate one-way NPT bound entangled features in case the conjecture is not true.

VII. ACKNOWLEDGMENTS

The author thanks Pawel Horodecki for fruitful discussions and critical comments on this paper. This work is supported by the ERC grant QOLAPS. Part of this work was performed at the National Quantum Information Center in Gdansk.

[1] A. C. Doherty, P. A. Parillo and F. M. Spedalieri, Phys. Rev. Lett. **88**, 187904 (2002) .
[2] A. C. Doherty, P. A. Parillo and F. M. Spedalieri, Phys. Rev. A **69**, 022308 (2004).
[3] B. M. Terhal, A. C. Doherty and D. Schwab, Phys. Rev. Lett. **90**, (2003).
[4] G. O. Myhr, N. Lütkenhaus, Phys. Rev. A **79**, 062307 (2009).
[5] G. O. Myhr et. al., Symmetric extensions in two-way quantum key distribution, Preprint quant-ph/0812.3607v1.
[6] T. Moroder, N. Lütkenhaus, Phys. Rev. A **74**, 052301 (2006).
[7] Jianxin Chen et. al, Phys. Rev. A **90**, 032318 (2014).
[8] I. Devetak and A. Winter, Proc. R. Soc. Lond. A **461**, 207 (2005).
[9] I. Devetak, A. Winter, Phys. Rev. Lett. **93**, 080501 (2004).
[10] K. Li, A. Winter,Squashed entanglement, k-extendibility, quantum Markov chains, and recovery maps, Preprint quant-ph/1410.4184 (2014).
[11] M. Curty, M. Lewenstein, N. Lütkenhaus, Phys. Rev. Lett.**92**, 217903 (2004).
[12] A. Jamiolkowski, Rep. Math. Phys. **3**, 275 (1972).
[13] W. Dur, G. Vidal, J.I. Cirac, Phys. Rev. A **62**, 062314 (2000) .
[14] K. Horodecki et al., Phys. Rev. Lett. **94**, 200501 (2005).
[15] K. Horodecki et al., Phys. Rev. Lett. **94**, 160502 (2005).
[16] R. Renner and S. Wolf, Advances in Cryptology - EUROCRYPT '03, Lecture Notes in Computer Science (2003).
[17] S. Hengl, J. Aberg and R. Renner, New J. Phys. **15**, 033025 (2013).
[18] M. L. Nowakowski, P. Horodecki, J. Phys. A: Math. Theor. **42**, 135306 (2009).
[19] M. L. Nowakowski, P. Horodecki, Phys. Rev. A **82**, 042342 (2010).
[20] S. Karnas, M. Lewenstein, J. Phys. A: Math. Gen. **34**, 6919 (2001).
[21] A. Milne, D. Jennings, S. Jevtic et al., Phys. Rev. A **90**, 1050-2947 (2014).
[22] M. Piani, Hierarchy of efficiently computable and faithful lower bounds to quantum discord, Preprint quant-ph/1501.06855.
[23] R. Quesada, A. Sanpera, Phys. Rev. A **89**, 052319 (2015).
[24] R. Alicki, M. Fannes, J. Phys. A **37**, L55 (2004).
[25] M. Christandl, A. Winter, IEEE Trans Inf Theory **51**, no 9, pp 3159-3165 (2005).
[26] M. Christandl and A. Winter, J. Math. Phys., 45(3), 29 (2004).
[27] F. Brandao, M. Christandl, Phys. Rev. Lett. **109**, 160502

(2012)
[28] G. Chiribella, Theory of Quantum Computation, Communication and Cryptography, 9 (Springer, 2011).
[29] O. Fawzi and R. Renner, Preprint quant-ph/1410.0664 (2014).
[30] F. G. Brandao, A. W. Harrow, J. Oppenheim and S. Strelchuk, Preprint quant-ph/1411.4921 (2014).
[31] R. Werner, Physical Review A **40**, 8 (1989).
[32] D. P. DiVincenzo, P. W. Shor, J. A. Smolin, B. M. Terhal and A. V. Thapliyal, Phys. Rev. A **61**, 062312 (2000).
[33] W. Dur, J. I. Cirac, M. Lewenstein, and D. Bru, Phys. Rev. A. **61**, p. 062313 (2000).
[34] G. Vidal, On the continuity of asymptotic measures of entanglement, Preprint quant-ph/0203107.